特許請求の範囲 (Claims)

1．　平文を受け付け、暗号化に用いる鍵から算出される拡大鍵をパラメタとして用いて攪拌を行い、得られる攪拌済の平文である攪拌文を更に繰り返し攪拌することで段階的に暗号化し、攪拌の最終段階より得られる攪拌文である暗号文に関しての強度の評価を行う暗号強度評価装置であって、

未攪拌文算出部と、制御部とを備えており、更に前記未攪拌文算出部が拡大鍵候補算出部と、未攪拌文算出部本体とを備えており、

前記未攪拌文算出部が、入力として前記平文と、攪拌の最終段階より得られる前記暗号文か、又はある中間段階より得られる前記攪拌文と推定される推定攪拌文とを受け付けるものであり、

前記拡大鍵候補算出部が、前記平文と、前記暗号文か、又は前記推定攪拌文とを用いて、当該段階での攪拌に用いられる前記拡大鍵と等しいと推定される一つの拡大鍵候補を算出するか、算出不能である場合は算出不能を示す算出不能識別データを出力し、また再算出を要求する再算出要求データを受け付けることで出力済の前記拡大鍵候補とは異なる新たな当該段階の前記拡大鍵候補を算出するものであり、

前記未攪拌文算出部本体が、前記拡大鍵候補と、前記暗号文か、又は前記推定攪拌文に基づいて当該段階で未だ攪拌されていない未攪拌文と等しいと推定される前記推定未攪拌文を算出し、前記未攪拌文算出部の出力として出力するものであり、

前記制御部が、対を成す前記平文と、攪拌の最終段階の前記暗号文又はある中間段階の前記推定攪拌文とを前記未攪拌文算出部へ入力し、出力される前記推定未攪拌文を受け付け当該段階の前段階の前記推定攪拌文として、前記平文と共に更に繰り返し前記未攪拌文算出部へ入力し、又、前記拡大鍵算出部より出力される前記算出不能識別データを受付けることで、前記再算出要求データを前記拡大鍵算出部へ出力し、前記拡大鍵算出部に再び前段階の新たな前記拡大鍵候補を算出させ、この新たな前記拡大鍵候補に基づいて前記推定未攪拌文

2．　平文を受け付け、暗号化に用いる鍵から算出される拡大鍵をパラメタとして用いて攪拌を行い、得られる攪拌済の平文である攪拌文を更に繰り返し攪拌することで段階的に暗号化し、攪拌の最終段階より得られる攪拌文である暗号文に関しての強度の評価を行う暗号強度評価装置であって、

未攪拌文算出部と、制御部とを備えており、更に前記未攪拌文算出部が拡大鍵候補算出部と、未攪拌文算出部本体とを備えており、

前記未攪拌文算出部が、入力として前記平文と、攪拌の最終段階より得られる前記暗号文か、又はある中間段階より得られる前記攪拌文と推定される推定攪拌文とを受け付けるものであり、

前記拡大鍵候補算出部が、前記平文と、前記暗号文か、又は前記推定攪拌文とを用いて、当該段階での攪拌に用いられるの拡大鍵と等しいと推定される拡大鍵候補を算出するために用いる条件を動的に構成し、前記条件に基づいて一つの前記拡大鍵候補を算出するか、算出不能である場合は算出不能を示す算出不能識別データを出力し、また再算出を要求する再算出要求データを受け付けることで出力済の前記拡大鍵候補とは異なる新たな当該段階の前記拡大鍵候補を算出するものであり、

前記未攪拌文算出部本体が、前記拡大鍵候補と、前記暗号文か、又は前記推定攪拌文に基づいて当該段階で未だ攪拌されていない未攪拌文と等しいと推定される前記推定未攪拌文を算出し、前記未攪拌文算出部の出力として出力するものであり、

前記制御部が、対を成す前記平文と、攪拌の最終段階の前記暗号文又はある中間段階の前記推定攪拌文とを前記未攪拌文算出部へ入力し、出力される前記推定未攪拌文を受け付け当該段階の前段階の前記推定攪拌文として、前記平文と共に更に繰り返し前記未攪拌文算出部へ入力し、又、前記拡大鍵算出部より出力される前記算出不能識別データを受付けることで、前記再算出要求データを前記拡大鍵算出部へ出力し、前記拡大鍵算出部に再び前段階の新たな前記拡大鍵候補を算出させ、この新たな前記拡大鍵候補に基づいて前記推定未攪拌文

3．　平文を受け付け、暗号化に用いる鍵から算出される拡大鍵をパラメタとして用いて攪拌を行い、得られる攪拌済の平文である攪拌文を更に繰り返し攪拌することで段階的に暗号化し、攪拌の最終段階より得られる攪拌文である暗号文に関しての強度の評価を行う暗号強度評価装置であって、

未攪拌文算出部と、制御部とを備えており、更に前記未攪拌文算出部が拡大鍵候補算出部と、未攪拌文算出部本体とを備えており、

前記未攪拌文算出部が、入力として前記平文と、攪拌の最終段階より得られる前記暗号文か、又はある中間段階より得られる前記攪拌文と推定される推定攪拌文とを受け付けるものであり、

前記拡大鍵候補算出部が、前記平文と、前記暗号文か、又は前記推定攪拌文とを用いて、当該段階での攪拌に用いられるの拡大鍵と等しいと推定される拡大鍵候補を算出するために用いる条件を動的に構成し、前記条件に基づいて一つの前記拡大鍵候補を算出するか、ある２つの前記条件が互いに矛盾することで前記拡大鍵候補の算出不能を識別し、算出不能を示す算出不能識別データを出力し、また再算出を要求する再算出要求データを受け付けることで出力済の前記拡大鍵候補とは異なる新たな当該段階の前記拡大鍵候補を算出するものであり、

前記未攪拌文算出部本体が、前記拡大鍵候補と、前記暗号文か、又は前記推定攪拌文に基づいて当該段階で未だ攪拌されていない未攪拌文と等しいと推定される前記推定未攪拌文を算出し、前記未攪拌文算出部の出力として出力するものであり、

前記制御部が、対を成す前記平文と、攪拌の最終段階の前記暗号文又はある中間段階の前記推定攪拌文とを前記未攪拌文算出部へ入力し、出力される前記推定未攪拌文を受け付け当該段階の前段階の前記推定攪拌文として、前記平文と共に更に繰り返し前記未攪拌文算出部へ入力し、又、前記拡大鍵算出部より出力される前記算出不能識別データを受付けることで、前記再算出要求データを前記拡大鍵算出部へ出力し、前記拡大鍵算出部に再び前段階の新たな前記拡

を出力させるものである暗号強度評価装置。

4．　平文を受け付け、暗号化に用いる鍵から算出される拡大鍵をパラメタとして用いて攪拌を行い、得られる攪拌済の平文である攪拌文を更に繰り返し攪拌することで段階的に暗号化し、攪拌の最終段階より得られる攪拌文である暗号文に関しての強度の評価を行う暗号強度評価装置であって、

第１未攪拌文算出部と、第２未攪拌文算出と、制御部とを備えており、更に第１未攪拌文算出部は未攪拌文算出部本体と、第１拡大鍵候補算出部とを備えたものであり、第２未攪拌文算出部は第２拡大鍵候補算出部を備えたものであり、

前記第１未攪拌文算出部が、入力として前記平文と、攪拌の最終段階より得られる前記暗号文か、又はある中間段階より得られる前記攪拌文と推定される推定攪拌文とを受け付けるものであり、

前記第２未攪拌文算出部が、入力として前記平文と、攪拌の最終段階より得られる前記暗号文か、又はある中間段階より得られる前記攪拌文と推定される推定攪拌文とを受け付けるものであり、

前記第１拡大鍵候補算出部が、前記平文と、前記暗号文か、又は前記推定攪拌文とを用いて、ある攪拌段階で用いられる前記拡大鍵の全探索を行い、当該段階での攪拌に用いられるの前記拡大鍵と等しいと推定される一つの拡大鍵候補を算出するか、算出不能である場合は算出不能を示す算出不能識別データを出力し、また再算出を要求する再算出要求データを受付けることで出力済の前記拡大鍵候補とは異なる新たな当該段階の前記拡大鍵候補を算出するものであり、

前記第２拡大鍵候補算出部が、前記平文と、前記暗号文か、又は前記推定攪拌文とを用いて、高階差分解読法を適用することで当該段階での攪拌に用いられるの前記拡大鍵と等しいと推定される拡大鍵候補を算出するために用いる複数の条件を動的に構成し、前記条件に基づいて一つの前記拡大鍵候補を算出するか、ある２つの前記条件が互いに矛盾することで前記拡大鍵候補の算出不

未攪拌文算出部本体が、前記拡大鍵候補と、前記暗号文か、又は前記推定攪拌文に基づいて当該段階で未だ攪拌されていない未攪拌文と等しいと推定される推定未攪拌文を算出し、未攪拌文算出部の出力として出力するものであり、

制御部が、対を成す前記平文と、攪拌の最終段階の前記暗号文又はある中間段階の前記推定攪拌文とを前記第１未攪拌文算出部へ入力し、出力される前記推定未攪拌文を受け付け当該段階の前段階の前記推定攪拌文として、前記平文と共に更に前記第２未攪拌文算出部へ入力し、又、前記第２拡大鍵算出部より出力される前記算出不能識別データを受け付けることで、前記再算出要求データを前記第１拡大鍵算出部へ出力し、前記第１拡大鍵算出部に再び前段階の新たな前記拡大鍵候補を算出させ、この新たな前記拡大鍵候補に基づいて前記推定未攪拌文を出力させるものである暗号強度評価装置。